

WHAT IS CLAIMED IS:

1 1. A method for performing data integration between two or more
2 computer systems provided over a network, the method comprising:
3 extracting data from a first database associated with a first computer system of
4 first type, the extracted data having a first file format and a first character-set format;
5 encrypting the data using a first security key;
6 storing the encrypted data in a shared volume provided in a storage system, the
7 storage system being coupled to a plurality of computer systems;
8 receiving the encrypted data from the shared volume of the storage system at a
9 second computer system of second type, the first and second computer system being of
10 different computer systems;
11 converting the received data from the first file format to a second file format,
12 the first file format being suitable for the first computer system and the second file format
13 being suitable for the second computer system;
14 decrypting the received data using a second security key that is associated with
15 the first security key; and
16 converting the received data from the first character-set format to a second
17 character-set format, the first character-set format being suitable for the first computer
18 system, the second character-set format being suitable for the second computer system.

1 2. The method of claim 1, wherein the first computer system is a
2 mainframe system, and the second computer system is an open system, and the plurality of
3 computer systems being associated with a plurality of different companies.

1 3. The method of claim 1, wherein the first file format is a counter key
2 data format.

1 4. The method of claim 3, wherein the second file format is a fixed block
2 architecture format.

1 5. The method of claim 1, wherein the first character-set format is an
2 Extended Binary Coded Decimal Interchange Code (EBCDIC) format.

1 6. The method of claim 1, wherein the second character-set format is an
2 American Standard Code for Information Interchange(ASCII) format.

1 7. The method of claim 1, wherein the first security key is a public key
2 associated with the second computer system, and the second security key is a private key
3 associated with the second computer system.

1 8. The method of claim 1, wherein the first security key is a private key
2 associated with the first computer system, and the second security key is a public key
3 associated with the first computer system.

1 9. The method of claim 1, wherein the first and second computer systems
2 are coupled to the storage system via a storage area network and the storage system includes
3 at least one disk array unit, wherein the first security key and the second security key are
4 common keys.

5 10. The method of claim 1, further comprising:
6 storing the encrypted data in a first volume of the storage system, the first
7 volume being associated with the first computer system,
8 wherein the plurality of computer systems are associated with a plurality of
9 different companies.

1 11. The method of claim 10, wherein the shared volume is configured to
2 be accessed only by computer systems of a given company, the first and second computer
3 systems being associated with the given company.

1 12. The method of claim 1, wherein the step of decrypting the received
2 data using a second security key is performed after the step of converting the received data
3 from the first file format to a second file format, and the step of converting the received data
4 from the first character-set format to a second character-set format is performed after the step
5 of decrypting the received data using a second security key.

1 13. The method of claim 1, further comprising:
2 generating a digital signature of the first computer system using the extracted
3 data;
4 transmitting the digital signature from the first computer system to the second
5 computer system;
6 receiving the digital signature at the second computer system; and

7 validating the received digital signature at the second computer system.

1 14. The method of claim 13, wherein the digital signature is transmitted
2 from the first computer system to the second computer system via a first communication link
3 that is different from a second communication link that is used to transfer the data from the
4 first computer system to the second computer system.

1 15. A method for performing data integration between two or more
2 computer systems provided over a network, the method comprising:

3 extracting data from a first database associated with a first computer system of
4 first type, the extracted data having a first format that is suitable for the first computer
5 system;

6 encrypting the data using a first security key; and

7 storing the encrypted data in a shared volume provided in a storage system, the
8 storage system being coupled to a plurality of computer systems associated with a plurality of
9 companies,

10 wherein the first security key is a public key of a second computer system, the
11 second computer system configured to handle data having a second format, wherein the first
12 format and the second format are different.

1 16. A method for sharing data between a plurality of computer systems
2 sharing a storage system, the method comprising:

3 receiving an encrypted data from a shared volume of the storage system at a
4 second computer system of second type, the encrypted data being data that has been extracted
5 from a first volume of the storage system that is associated with a first computer system of
6 first type;

7 converting the received data from a first format to a second format, the first
8 format being suitable for the first computer system and the second format being suitable for
9 the second computer system;

10 decrypting the received data using a second security key that is associated with
11 a first security key that has been used to encrypt the extracted data at the first computer
12 system; and

13 thereafter, loading the data to a second volume of the storage system, the
14 second volume being associated with the second computer system.

1 17. The method of claim 16, further comprising:
2 converting the received data from a third format to a fourth format, the third
3 format being suitable for the first computer system, the fourth format being suitable for the
4 second computer system.

1 18. The method of claim 17, wherein the first format is a file format of
2 first type, and the second format is a file format of second type.

1 19. The method of claim 17, wherein the third format is a character-set of
2 first type, and the fourth format is a character-set of second type.

1 20. The method of claim 19, wherein the step of converting the received
2 data from a third format to a fourth format is performed after the step of decrypting the
3 received data using a second security key, and the step of decrypting the received data using a
4 second security key is performed after the step of converting the received data from a first
5 format to a second format.

1 21. The method of claim 16, further comprising:
2 receiving a digital signature of the first computer, the digital signature being
3 associated with the received data; and
4 authenticating the digital signature of the first computer system.

1 22. The method of claim 21, wherein the digital signature is received via a
2 local area network and the data is received via a storage area network.

1 23. A computer system, comprising:
2 an interface for coupling with a storage system; and
3 a computer storage medium including:
4 code for receiving an encrypted data from a shared volume of the
5 storage system, the encrypted data being data extracted from a first volume of the storage
6 system that is associated with another computer system that is different than the computer
7 system,
8 code for converting the received data from a first format to a second
9 format, the first format being suitable for the another computer system and the second format
10 being suitable for the computer system,

11 code for decrypting the received data using a second security key that
12 is associated with a first security key that has been used to encrypt the extracted data at the
13 another computer system, and

14 code for loading the data to a second volume of the storage system, the
15 second volume being associated with the computer system.

1 24. A computer readable medium, comprising:

1 code for receiving an encrypted data from a shared volume of the storage
2 system at a second computer system of second type, the encrypted data being data extracted
3 from a first volume of the storage system that is associated with a first computer system of
4 first type;

5 code for converting the received data from a first format to a second format,
6 the first format being suitable for the first computer system and the second format being
7 suitable for the second computer system;

8 code for decrypting the received data using a second security key that is
9 associated with a first security key that has been used to encrypt the data at the first computer
10 system; and

11 code for loading the data to a second volume of the storage system, the second
12 volume being associated with the second computer system.

1 25. The computer readable medium of claim 24, wherein the first and
2 second security keys are associated with a Public Key Cryptography standard or Common
3 Key standard.